ABSTRACT

The secure messaging system of the invention encrypts an electronic document using a symmetric key and transmits the encrypted document and related message parameters to a recipient whose identity is then authenticated by a web server. The web server dynamically regenerates the symmetric key from a hidden key and from the message parameters accompanying the encrypted document, and thus avoids having to maintain a central repository of encrypted documents as required by typical "post and pick-up" encrypted messaging systems. Further, an audit trail produced while practicing the invention provides timestamped message digest data for a plurality of time intervals, where the message digests for adjacent time intervals are computationally linked together. The audit trail effectively enables timestamped message digest data to verify not only the existence of a document during a first time interval, but also to verify the existence of documents encountered in a prior time interval.